2017 9th International Conference on Cyber Conflict
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)

From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law

Kubo Mačák
Law School
University of Exeter
Exeter, United Kingdom
k.macak@exeter.ac.uk

Abstract: The law of war was famously described by Sir Hersch Lauterpacht as being 'at the vanishing point of international law'. However, in a historical twist, international legal scrutiny of cyber operations emerged and developed precisely through the optics of the law of war. This paper analyses the influence that the development of the cyber law of war has had and might yet have on the 'core' of international law, in other words, on general international law. It analyses three key dimensions of the relationship between the law of war and general international law: systemic, conceptual, and teleological. It argues that, firstly, a systemic-level shift has taken place in the discourse, resulting in the academic debate and state focus moving from law-of-war questions to questions of general international law including sovereignty, non-intervention, and state responsibility. A better understanding of this trend should allay the fears of fragmentation of international law and inform the debate about the relationship between the law of war and 'core' international law. Secondly, this development has created fertile grounds for certain concepts to migrate from the law of war, where they had emerged, developed or consolidated, into general international law. A case in point is the functionality test, which originated as a compromise solution to determine whether a cyber operation amounts to an 'attack' under the law of war, but which may offer additional utility in other areas of international law including the law of state sovereignty and the law of arms control and disarmament. Thirdly, however, it is imperative that the unique teleological underpinning of the law of war is taken into consideration before introducing its rules and principles to different

normative contexts. Paradoxically, a blanket transplantation of these norms might in practice jeopardise the underlying humanitarian considerations.

Keywords: *cyber attacks, cyber security, functionality test, general international law, law of war*

1. INTRODUCTION

Described in the press as 'the year of the hack',[1] 2016 was anything but short on major cyber security incidents. The technology company Yahoo! revealed that more than one billion of its user accounts had been compromised.[2] Three US intelligence agencies suggested in a joint report that the current Russian leadership had ordered specific cyber operations with the intent to interfere with the 2016 presidential election in favour of Donald Trump.[3] Dwarfing all other incidents in terms of its immediate impact, a DDoS attack against the internet infrastructure provider Dyn made dozens of major internet platforms and services inaccessible across the world.[4]

Although the prominence of these attacks can hardly be disputed, there have been no serious claims that any of them should be viewed as an act of war or perceived through the lens of the regulation of warfare on the international plane. It appears that the 'military paradigm' is now firmly on the decline when it comes to analysing malicious cyber operations from the perspective of international law. The bold prediction from a few years ago that 'Cyber War Will Not Take Place' in an eponymous article by Thomas Rid[5] seems to have held water. But does that mean the law of war has nothing to offer to general international law with respect to the regulation of cyber operations?[6]

1 Geof Wheelwright, 'How 2016 Became the Year of the Hack – and What it Means for the Future' *The Guardian* (21 December 2016) <https://www.theguardian.com/technology/2016/dec/21/how-2016-became-the-year-of-the-hack-and-what-it-means-for-the-future>.

2 'Important Security Information for Yahoo Users' *Business Wire* (14 December 2016) <http://www.businesswire.com/news/home/20161214006239/en/Important-Security-Information-Yahoo-Users>.

3 United States (US), Office of the Director of National Intelligence, 'Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution' (6 January 2017) <https://www.dni.gov/files/documents/ICA_2017_01.pdf>.

4 Nicky Woolf, 'DDoS attack that disrupted internet was largest of its kind in history, experts say' *The Guardian* (26 October 2016) <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>.

5 Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35 Journal of Strategic Studies 5. An extended version of the argument was published as Thomas Rid, *Cyber War Will Not Take Place* (OUP 2013).

6 For the purposes of this paper, the term 'law of war' is understood as 'that part of international law that regulates the resort to armed force; the conduct of hostilities and the protection of war victims in both international and non-international armed conflict; belligerent occupation; and the relationships between belligerent, neutral, and non-belligerent States'. US Department of Defense, *Law of War Manual* (2015). The term 'general international law' has been authoritatively defined as 'that which is binding upon a great many states. General international law, such as provisions of certain treaties which are widely, but not universally, binding and which establish rules appropriate for universal application, has a tendency to become universal international law'. Robert Jennings and Arthur Watts, *Oppenheim's International Law* (9th edn., OUP 2008) 4.

This paper challenges the assumption belying that rhetorical question. A point of historical irony ought to be highlighted at the outset. To borrow from Sir Hersch Lauterpacht's famous statement, the law of war has long been seen as confined to 'the vanishing point of international law'.[7] Yet, in an unexpected twist, international legal scrutiny of cyber operations emerged and developed precisely through the optics of the law of war. And that is the background against which the paper argues for particular effects which the law at the 'vanishing point' has had, may yet have, but also ought not to have on the 'core' of international law.

The paper commences by analysing the development of the cyber law of war and the corresponding gradual systemic shift of the discourse towards areas of international law closer to its core (Section 2). It then examines the conceptual dimension of the relationship between the law of war and general international law by focussing on the 'functionality test' as a concept arising in the former area and on its potential and actual impact on the latter (Section 3). Finally, it warns that the unique teleological underpinning of the law of war must be taken into consideration before transplanting its rules and principles to different normative contexts more generally (Section 4).

2. SYSTEMIC DIMENSION

Traditionally, international law maintained a strict division between war and peace. Since Ciceronian times,[8] it has been said that *inter bellum et pacem nihil est medium*: there was no intermediate state between war and peace.[9] This meant that international law was in fact a composite of two disparate bodies of rules. There was one set of norms for the peacetime (the law of peace) and another one that applied in times of war (the law of war). The orthodox view was that there was no status mixtus under international law: each situation was either one of peace or war, and the corresponding body of law would apply to it exclusively.[10]

That is no longer true today.[11] For a number of reasons – which include the existence of a multitude of actors on the international plane, the complexity of relations in the globalised world, as well as the asymmetrical nature of most contemporary armed conflicts – norms that used to be clumped together as 'peacetime law' now do not cease to apply with the outbreak of hostilities. This has been recognised expressly by the International Court of Justice (ICJ) with respect to a central area of the law of peace, namely international human rights law.[12] In a situation of armed conflict, the two originally separate bodies of law now apply in parallel,[13]

7 Hersch Lauterpacht, 'The Problem of the Revision of the Law of War' (1952) 29 British Year Book of International Law 360, 382.

8 Cicero, *Philippics 3–9* (Gesine Manuwald tr, Walter de Gruyter 2007) vol I, 260.

9 Hugo Grotius, *The Law of War and Peace in Three Books* (Francis W Kelsey tr, 1625) book III, ch XXI, s I, §1.

10 Robert Joseph Phillimore, *International Law* (Butterworths 1879) vol III, 794.

11 Aoife O'Donoghue, 'Splendid Isolation: International Humanitarian Law, Legal Theory and the International Legal Order' (2011) 14 *Yearbook of International Humanitarian Law* 107, 114; Jann K Kleffner, 'Scope of Application of International Humanitarian Law' in Dieter Fleck (ed.) *The Handbook of International Humanitarian Law* (3rd edn., OUP 2013) 70.

12 ICJ, Legality of the Threat or Use of Nuclear Weapons Case (Advisory Opinion) [1996] ICJ Rep 226 [24]–[25] ('Nuclear Weapons Advisory Opinion'); ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136 [106].

13 Cf. UN, Human Rights Committee, General Comment No. 31, UN Doc CCPR/C/21/Rev.1/Add. 13 (26 May 2004) ('both spheres of law are complementary, not mutually exclusive').

and any norm conflict is resolved (or, as the case may be, avoided) by the applicable maxims of interpretation (including the central principle of *lex specialis derogat legi generali*).[14]

However, not all traces of the historical distinction have disappeared. It is true that general international law and its norms concerning state responsibility, treaty interpretation or identification of custom apply equally during armed hostilities and in times of peace. However, norms governing the use of armed force have maintained their conceptual separation from the rest of international law. These norms comprise mainly the *jus ad bellum* and the *jus in bello*: the former sets out conditions under which states may resort to war, the latter provides rules which the belligerents must abide by once they are engaged in an armed conflict.[15] Crucially, neither of these bodies of law applies to situations not characterised by any use of armed force. Therefore, the radically different optics of rules applicable during peacetime and those applicable to uses of armed force are still very much present in modern international law.

In this sense, international legal scrutiny of cyber operations initially emerged and developed through the optics of the law of war, and not the law of peace. The first analyses came in the form of academic writings in the late 1990s, which considered cyber conflict as a species of armed conflict.[16] The risk of a 'Cyber Pearl Harbor' or a 'Cyber Armageddon', a hypothetical devastating cyber attack against state infrastructure, was envisaged for the first time in the same period.[17] (Today, nearly two decades later, such incidents belong only in the realm of journalists' and novelists' imaginations,[18] and the likelihood of their happening in reality is seen as extremely low.[19]) Against this background, scholars considered what degree of 'computer network attack' would qualify as a use of force under Article 2(4) of the UN Charter.[20]

Early state reactions were similar in their scope and approach. For instance, a prescient 1999 memo by the United States (US) Department of Defense expressly noted that '[t]he law of war is probably the single area of international law in which current legal obligations can be applied with the greatest confidence to information operations'.[21] Another prominent statement by the US, the 2011 *International Strategy for Cyberspace*, went even further and warned that the

14 See further Matthew Happold, 'International Humanitarian Law and Human Rights Law' in Nigel D White and Christian Henderson (eds.), *Research Handbook on International Conflict and Security Law* (Edward Elgar 2012) 459–463; Marko Milanovic, 'The Lost Origins of *Lex Specialis*: Rethinking the Relationship between Human Rights and International Humanitarian Law' in Jens David Ohlin (ed.), *Theoretical Boundaries of Armed Conflict and Human Rights* (CUP 2016) 103–113.

15 See, e.g., Christopher Greenwood, 'The Relationship Between *Ius ad Bellum* and *Ius in Bello*' (1983) 9 *Review of International Studies* 221.

16 See, e.g., Richard W Aldrich, 'The International Legal Implications of Information Warfare' (1996) 10 Airpower Journal 99; Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885.

17 See, e.g., Pierre Thomas, 'Experts Prepare for "An Electronic Pearl Harbor"' CNN (7 November 1997) <https://archive.is/aL98j>.

18 See, e.g., Mark Russinovich, *Zero Day* (Corsair 2012).

19 Sean Lawson, 'Does 2016 Mark the End of Cyber Pearl Harbor Hysteria?' *Forbes* (7 December 2016) <http://www.forbes.com/sites/seanlawson/2016/12/07/does-2016-mark-the-end-of-cyber-pearl-harbor-hysteria/>.

20 See, e.g., Todd A Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 *Case Western Reserve Journal of International Law* 567; Mark R Jacobson, 'War in the Information Age: International Law, Self-Defense, and the Problem of 'Non-Armed' Attacks' (1998) 21 *Journal of Strategic Studies* 1; Schmitt (n 16).

21 US, Department of Defense, 'An Assessment of International Legal Issues in Information Operations' (May 1999) 11.

US would respond to hostile acts in cyberspace in line in accordance with its inherent right to self-defence.[22] In the interim, other states either remained silent or endorsed a similar approach.

With hindsight, the 2007 cyber attacks against Estonia stand out as a watershed event for international cyber security law. That year, a decision to remove a Soviet-era sculpture of a Red Army soldier from a central square in the capital city Tallinn[23] led to a concentrated series of cyber operations against a multitude of public and private targets across the country.[24] While the events were unfolding, Estonia even described itself as 'under attack' by Russia.[25] In the aftermath of the incident, NATO established the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn.[26] Much of the early work of the CCD COE, of which the most prominent was the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, maintained the law-of-war focus on the regulation of cyberspace.[27]

The *Tallinn Manual* itself dedicated nearly 90% of its rules to the *jus ad bellum* and the *jus in bello*.[28] The remaining ones were reportedly added in the final stages of editing to provide a general context and to underscore the continued application of general international law even in times of (cyber) conflict.[29] Somewhat paradoxically, given the origins of the project, the international group of experts concluded that the attacks against Estonia in 2007 did not reach the threshold of an armed attack or armed conflict and therefore fell outside the scope of the law of war.[30] Nonetheless, the attacks have remained a prime reference point and a trigger for much legal development in the area of cyber security.

To some extent, the predominant law-of-war focus of all of these developments is certainly understandable. Notably, this progression mirrors the development of the Internet, which also started as a military project in the US. It is also undoubtedly related to states' general preoccupation with national security and the high priority that many governments accord to military defence against foreign threats. Last but not least, the military focus has in large part been caused by the fact that a lot of thinking on cyber security within governments was originally done within military and defence circles.[31]

22 US, The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (2011) 9.

23 Steven Lee Myers, 'Estonia removes Soviet-era war memorial after a night of violence' *The New York Times* (27 April 2007) <http://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html>.

24 See further Eneken Tikk, Kadri Kaska, and Liis Vihul, International Cyber Incidents: Legal Considerations (CCD COE 2010) 18–24.

25 'Statement by the Foreign Minister Urmas Paet' Eesti Päevaleht (1 May 2007) <http://epl.delfi.ee/news/eesti/statement-by-the-foreign-minister-urmas-paet?id=51085399> ('The European Union is under attack, because Russia is attacking Estonia').

26 'NATO Opens New Centre of Excellence on Cyber Defence' *NATO News* (14 May 2008) <http://www.nato.int/docu/update/2008/05-may/e0514a.html>. It should be noted that the concept for a cyber defence centre was submitted by Estonia to NATO already in 2004. It was subsequently approved by the Supreme Allied Commander Transformation in 2006. See NATO CCD COE, 'History' (undated) <https://ccdcoe.org/history.html>.

27 Michael N Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013).

28 Id., rules 10–95.

29 Michael J Adams, 'A Warning About Tallinn 2.0 … Whatever It Says' *Lawfare* (4 January 2017) <https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says>.

30 *Tallinn Manual* (n 27) 57–58 and 75.

31 See further Kenneth Geers, *Strategic Cyber Security* (CCD COE 2011) 19–32.

However, this approach has also led to serious concerns about the downsides of applying the so-called 'military paradigm' to international legal regulation of cyberspace. These concerns have been voiced by several western academics,[32] but – perhaps more importantly – also by non-Western states led by China.[33] According to such critical views, the key risk of the law of war focus on the regulation of cyberspace was that it would 'aggravate the arms race and militarisation in cyberspace'.[34] This fundamental difference in approach to the rule of law in cyberspace between the West and 'the Rest' led by China and Russia has been reflected in commentators' references to two competing 'camps' of states as far as cyber security is concerned.[35]

It would be hasty to equate the question of applicability of the law with the threat of militarisation of cyberspace. As the ICRC stated in a 2015 report to the 32nd International Conference of the Red Cross and Red Crescent:

> [A]sserting that IHL applies to cyber warfare is not an encouragement to militarize cyberspace and should not, in any way, be understood as legitimizing cyber warfare.[36]

This is an obvious truth. Similarly, it would be manifestly wrong to claim that an assertion that Geneva Conventions apply somehow legitimises warfare in general.[37]

Still, the worries about the creeping militarisation of cyberspace cannot easily be brushed away. In the concluding remarks of a 2014 monograph dedicated to a close scrutiny of cyber operations from the perspective of international law, Professor Marco Roscini made the following striking summation: '[t]he militarization of cyberspace is not a risk, it is already a fact'.[38] This state of affairs has some obvious negative consequences. It has been well documented that framing cyber threats as strategic-military concerns contributes to the creation of an 'atmosphere of insecurity and tension in the international system'.[39]

However, a closer look reveals a paradox at the heart of the issue. The originally predominant law-of-war approach based on the viewing of threats to cyber security through the prism of

32 See, e.g., Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17 *Journal of Conflict and Security Law* 187; Robin Geiss and Henning Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention', in Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE 2013).

33 Ma Xinmin, 'Key Issues and Future Development of International Cyberspace Law' (2016) 2 *China Quarterly of International Strategic Studies* 119, 128.

34 Ibid.

35 See, e.g., Scott Shackleford and Amanda Craig, 'Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity' (2014) 50 *Stanford Journal of International Law* 119, 135; Kristen Eichensehr, 'The Cyber-Law of Nations' (2015) 103 Georgetown Law Journal 317, 333; Nigel Inkster, *China's Cyber Power* (Routledge 2015) 9.

36 ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (October 2015) <https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf > 40.

37 See Gabor Rona, 'Challenges New Weapons and Humanitarian Assistance Present for International Law' *Just Security* (20 November 2015) <https://www.justsecurity.org/27789/challenges-weapons-humanitarian-assistance-present-ihl/>.

38 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 280.

39 Myriam Dunn Cavelty, 'The Militarisation of Cyberspace: Why Less May Be Better' in C Czosseck, R Ottis, K Ziolkowski (eds.), *2012 4th International Conference on Cyber Conflict* (NATO CCD COE 2012) 141.

strategic or military discourse does not actually correspond to reality. In fact, most cyber operations either fall below the threshold of armed conflict, or do not occur in the context of an armed conflict, or even if they do, they fail to be attributable to a state or to bring about a sufficiently serious effect.[40] As such, the framework of the law of war is not applicable to the vast majority of the existing cyber operations.

Gradually, key actors have recognised that to resolve this paradox, cyber operations must indeed be analysed outside the 'military paradigm'.[41] This has led to a systemic shift in the discourse, with academic debate and state focus migrating from law-of-war questions to questions of general international law including sovereignty, non-intervention, and state responsibility. Among scholars, this shift was reflected in criticism levied against the method and remit of the *Tallinn Manual* as a perceived leading example of the militarisation trend.[42] To their credit, the international group of experts responded by enlarging the scope of the project to include 'below the threshold' cyber operations.[43] As acknowledged by Professor Michael Schmitt, the project director, 'preoccupation with cyber armed attacks is counter-experiential'.[44] The second edition of the Manual, which has just been published, reflects this shift in the discourse and includes a discussion of state responsibility, the law of the sea, air and space law, and even human rights law.[45]

Similarly, states have moved away from the military paradigm in their recent conduct and official statements. One overarching example is the ongoing work of the United Nations (UN) Group of Governmental Experts (GGE), which has so far resulted in the adoption of three substantive reports.[46] These reports are based on the official submissions of the most cyber-active states and are adopted by consensus of all representatives.[47] To the extent that they have related to international law (as opposed to political norms of conduct in cyberspace), these references have almost exclusively maintained the perspective of peacetime law.[48] A similar trend can be observed at the level of individual states. Even the US, as the supposed principal proponent of the military paradigm, has modified its approach. For example, in late 2016, Brian Egan, the US State Department Legal Adviser, delivered a landmark speech on 'International

40 See, e.g., Tikk, Kaska, and Vihul (n 24) 82–83 ('it is highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks – the objective evidence of the case is too vague to meet the necessary criteria of both state involvement and gravity of effect').

41 See, e.g., Oona A Hathaway et al., 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817, 840; Geiss and Lahmann (n 32) 657; Michael N Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' (2014) 54 *Virginia Journal of International Law* 697, 698.

42 See, e.g., Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New *Tallinn Manual*' (2013) 18(2) *Journal of Conflict and Security Law* 331, 332–335; Kristen Eichensehr, 'Review of The *Tallinn Manual* on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013)' (2014) 108 *American Journal of International Law* 585, 589; Ma Xinmin, 'Letter to the Editors: What Kind of Internet Order Do We Need?' (2015) 14 *Chinese Journal of International Law* 399, 402.

43 Jill Dougherty, 'NATO Cyberwar Challenge: Establish Rules of Engagement' CNN (7 November 2016) <http://edition.cnn.com/2016/11/07/politics/nato-cyber-centre-international-law/>.

44 Schmitt (n 41) 698.

45 Michael N Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., CUP 2017).

46 UN Doc A/65/201 (2010); UN Doc A/68/98 (2013); UN Doc A/70/174 (2015).

47 See further UN, 'Developments in the Field of Information and Telecommunications in the Context of International Security' (undated) <https://www.un.org/disarmament/topics/informationsecurity/>.

48 But see UN Doc A/65/201 (2010) para 7; UN Doc A/70/174 (2015) para 28(d).

Law and Stability in Cyberspace'.[49] Although the speech did contain a brief section on cyber operations in the context of armed conflict,[50] the vast majority of the text was devoted to peacetime aspects of cyberspace regulation.[51]

Therefore, an examination of the systemic dimension of the relationship between the law of war and general international law reveals a clear shift of focus from the former to the latter, as far as the international regulation of cyber operations is concerned. This has had two main consequences. First, the transition of the debate from one specific area of international law – the law of war – to general international law demonstrates that concerns about a supposed fragmentation of international law may in fact be less salient than some have worried.[52] Secondly, this systemic shift has allowed for concepts and approaches to migrate from the law of war to general international law. The next two sections explore the opportunities and limitations posed by this particular migratory pattern.

3. CONCEPTUAL DIMENSION

The conceptual level of the relationship between the law of war and general international law reveals the potential for certain ideas, concepts or approaches to migrate from the former into the latter. Given the limited scope of the paper, this section focusses on one particular issue, namely the conceptualisation of the non-physical effects of cyber operations in international law.[53] Unsurprisingly, this question acquires central importance in relation to cyber security. Unlike ordinary conduct in the physical world, cyber operations result in effects that are normally invisible to the naked eye. At what point do they then become relevant from the perspective of the law?

In the law of war, this question arises in the context of the regulation of targeting. This area of the law is based on the principle of distinction, codified in Article 48 of Additional Protocol I (AP I), described by the ICJ as one of the 'cardinal principles' of the law of war,[54] and generally considered to reflect customary law.[55] This provision mandates that belligerents must at all times distinguish 'between civilian objects and military objectives and accordingly [must] direct their operations only against military objectives'.[56]

49 Brian J Egan, 'International Law and Stability in Cyberspace' (10 November 2016) <www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf>.

50 Id., 8–10.

51 Id., 1–8 and 11–26.

52 See Martti Koskenniemi and Päivi Leino, 'Fragmentation of International Law? Postmodern Anxieties' (2002) 15 *Leiden Journal of International Law* 553.

53 Other conceptual questions at the intersection between the law of war and general international law include the geographical scope of applicability of the law in relation to cyberspace; the requirement of organisation in online groups; or the problem of calculating proportionality *largo sensu* in the cyber context.

54 Nuclear Weapons Advisory Opinion (n 12) [78].

55 Id. [79]; Eritrea-Ethiopia Claims Commission, Partial Award, Western Front, Aerial Bombardment and Related Claims, Eritrea's Claims 1, 3, 5, 9–13, 14, 21, 25 & 26 (2005) 26 RIAA 291, 327; Jean-Marie Henckaerts and Louise Doswald-Beck (eds.), *Customary International Humanitarian Law* (CUP 2005) 3.

56 Article 48 AP I.

There is some discussion as to the precise meaning of the term 'operations' (or, in full, 'military operations'[57]) in the cited provision for the purposes of the law of war. Some believe that it is practically synonymous with the notion of 'attack' used in almost all specific rules on targeting in the same section of the Protocol.[58] Others consider 'attacks' to be a subset of 'military operations'.[59] According to this latter view, activities such as moving armed forces, gathering military intelligence or providing logistical support qualify as military operations, but not as 'attacks' *stricto sensu*. Nevertheless, for our present purposes, it will suffice to focus on the concept of 'attack' as it is the central threshold notion of the law of targeting.

Accordingly, it is by reference to that notion that we determine whether the relevant targeting rules apply to a particular combat action against the enemy. If the conduct in question is an 'attack', then it must conform to these rules, which include the prohibition of attacks against civilians and civilian objects,[60] the prohibition of indiscriminate attacks,[61] and the prohibition of attacks causing disproportionate 'collateral' damage to civilians or civilian property.[62] This conclusion, however, invites the question how to determine whether a given cyber operation qualifies as an 'attack'.

Although the first Additional Protocol provides a widely accepted definition of that term, its precise application to cyber operations is controversial. According to Article 49(1) AP I, '"[a]ttacks" means acts of violence against the adversary, whether in offence or in defence'. Despite the reference to violence, '[t]he use of physical force is not a *sine qua non* of an attack under the terms of the Protocol'.[63] Yet the spectrum of views concerning which cyber operations would qualify accordingly is very broad.

At the one end of the spectrum, the requirement of violence is interpreted as meaning that 'attack' only includes those operations which result in injury or death to individuals or damage or destruction of physical objects.[64] On this view, an operation aimed at temporarily disabling a device or a network – for instance, by shutting down an electrical distribution grid[65] – would not qualify as an 'attack'.[66] At the other extreme, it was argued that cyber operations with reversible effects should be seen as 'neutralising' an object,[67] and as such they would qualify as

57 See Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds.) Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (ICRC 1987) 600.

58 See, e.g., Michael N Schmitt, 'Wired Warfare: Computer Network Attack and *Jus in Bello*' (2002) 84 *International Review of the Red Cross* 365, 376; David Turns, 'Cyber War and the Concept of 'Attack' in International Humanitarian Law' in Dan Saxon (ed.) *International Humanitarian Law and the Changing Technology of War* (Brill 2013) 217; Roscini (n 38) 178.

59 See, e.g., Michael Bothe, Karl Josef Partsch and Waldemar A Solf (eds.), *New Rules for Victims of Armed Conflicts: Commentary on the two 1977 Protocols Additional to the Geneva Conventions of 1949* (Martinus Nijhoff 1982) 408; UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (OUP 2004) 81 fn 187; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 199.

60 Article 51(2) AP I.

61 Article 51(4) AP I.

62 Article 51(5)(b) AP I.

63 Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 *Israel Law Review* 55, 76.

64 Schmitt (n 58) 374.

65 Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks' <https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf> 4.

66 Schmitt (n 58) 374.

67 The 'neutralisation' of an object is one of the modalities of enemy engagement foreseen by Article 52(2) AP I and therefore, the argument goes, a form of 'attack'.

'attacks'.[68] Consequently, an operation against the electric grid mentioned above would be an 'attack' even if its aim was merely to disable it, and not to cause its destruction.

Professor Schmitt documented how the discussions in the context of the *Tallinn Manual* project resulted in the adoption of a new, compromise position between the two extremes in the form of a 'functionality test'.[69] As expressed in both editions of the *Manual*, this test mandates that 'interference by cyber means with the functionality of an object constitutes damage or destruction'[70] and as such it amounts to an 'attack'.[71] Although there were some shades of difference among the experts as to the precise meaning of interference,[72] the majority of them agreed that the criterion would be met if, as a result of a cyber operation, 'the object in question is unusable for its intended purpose, at least until some form of repair is undertaken'.[73] Hence, the operation against the electric grid would qualify as an attack if it either made the grid permanently inoperable or necessitated some degree of repair.[74]

Crucially, this functionality-oriented approach towards the definition of a cyber attack can have impact on other areas of international law closer to its core. Two specific observations can be made in this regard. Firstly, the functionality test directly influences what is to be considered as a 'weapon', which is a term that exceeds the boundaries of the law of war. This is because 'cyber capabilities that are used, designed, or intended to be used' for the purposes of 'attacks' in the sense of Article 49(1) AP I, are 'cyber weapons to which the law of weaponry applies'.[75] Accordingly, a cyber tool that may cause loss of functionality of an object is subject to the prescriptions of weapons law, a body of law that includes, in addition to the law of war rules, the law of arms control and disarmament.[76] As it is well established that states must refrain from using 'weapons' against civil aircraft in flight,[77] the functionality test may also have further influence even on international civil aviation law.[78] It should be noted that prominent official as well as scholarly definitions of 'cyber weapons' align with this functionality-oriented interpretation.[79]

Secondly, the functionality test has proven capable of application in other areas of international law. The discussions in the Tallinn 2.0 process have led to an agreement among the international

68 ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (October 2011) <https://app.icrc.org/e-briefing/new-tech-modern-battlefield/media/documents/4-international-humanitarian-law-and-the-challenges-of-contemporary-armed-conflicts.pdf> 37.

69 Michael N Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (2014) 96 *International Review of the Red Cross* 189, 198–201.

70 *Tallinn Manual* (n 27) 108; *Tallinn Manual 2.0* (n 45) 417.

71 *Tallinn Manual* (n 27) 108–109; *Tallinn Manual 2.0* (n 45) 417.

72 See *Tallinn Manual* (n 27) 108–109 paras 10 and 11; see further *Tallinn Manual 2.0* (n 45) 417–418 paras 10–12.

73 Schmitt (n 69) 199.

74 *Tallinn Manual* (n 27) 108–109; *Tallinn Manual 2.0* (n 45) 417.

75 William H Boothby, *Weapons and the Law of Armed Conflict* (2nd edn., OUP 2016) 238; see also *Tallinn Manual* (n 27) 141–142; *Tallinn Manual 2.0* (n 45) 452–453.

76 Boothby (n 75) 2–3.

77 Convention on International Civil Aviation (signed at Chicago on 7 December 1944) 15 UNTS 295 ('Chicago Convention'), as amended by the Protocol Relating to an Amendment to the Convention on International Civil Aviation (signed at Montreal on 10 May 1984), Article 3*bis*(a) ('every State must refrain from resorting to the use of weapons against civil aircraft in flight').

78 See further *Tallinn Manual 2.0* (n 45) 268–269.

79 See, e.g., US, Department of the Air Force Instruction 51-402, Legal Reviews of Weapons and Cyber Capabilities (27 July 2011) 6, incorporated by reference in *US Law of War Manual* (n 6) 999 fn 75; Thomas Rid and Peter McBurney, 'Cyber Weapons' (2012) 157 *RUSI Journal* 6, 7.

group of experts that state-sponsored cyber operations that result in the loss of functionality of cyber infrastructure on the territory of another state without its consent may amount to a violation of that state's sovereignty.[80] It also reflects a broader development in the international community and states' general approach to the regulation of cyberspace. For instance, in a submission to the UN GGE, Panama expressly described operations restricted to cyberspace as a 'new form of violence'.[81] More recently, the US State Department Legal Advisor Brian Egan expressly stated that 'one state's non-consensual cyber operation in another state's territory could violate international law, even if it falls below the threshold of a use of force'.[82] The functionality test may provide the much-needed granularity to such generalised and open-ended official proclamations.

4. TELEOLOGICAL DIMENSION

The foregoing discussion might suggest that it is tempting to search for as many notions and approaches at the interface of the law of war and general international law as possible. Admittedly, a legal standard like the functionality test may bring additional granularity to currently less developed areas of international cyber security law. However, we should be wary of transplanting law-of-war notions and approaches without closer scrutiny. Particularly, we must not lose sight of the unique teleological underpinning of the law of war, which sets it apart from other disciplines of international law.

The teleology of the law of war is 'predicated on a subtle equilibrium between the two diametrically opposed stimulants of *military necessity* and *humanitarian considerations*'.[83] This means that most of its rules are based on an inbuilt balance between these two keystone values. For instance, the principle of proportionality in targeting permits attacks against lawful targets (thus allowing conduct that is militarily necessary), but only up to that abstract point at which the expected collateral damage of the attack outweighs the anticipated military advantage (thus disallowing such attacks for humanitarian reasons).[84] It is because of this equilibrium unique to the law of war that notions and approaches developed in its context cannot be automatically transplanted to domains where one or both of the stimulants are absent.

This is an important warning, as calls for the wholesale adoption of law-of-war approaches to decision-making about cyber defence generally have already started appearing in the literature.[85] To some extent, this development is understandable because the law of war may seemingly offer a ready-made detailed legal framework which has been extensively mulled over in relation to cyber operations. The key implication of such proposals is that the permissibility of a specific cyber operation would be determined by a *mutatis mutandis* application of the law-of-war principles of targeting, including distinction, precautions in attack, and proportionality.

80 *Tallinn Manual 2.0* (n 45) 20–21.
81 UN Doc A/57/166/Add.1 (29 August 2002) 5.
82 Egan (n 49) 13.
83 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn., CUP 2016) 9 (emphases added).
84 Articles 51(5)(b), 57(2)(a)(iii), and 57(2)(b) AP I.
85 See, e.g., Corey T Holzer and James E Lerums, 'The Ethics of Hacking Back' (2016) <https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2016-01.pdf>.

However, it is submitted that if a cyber operation takes place outside of the context of an armed conflict or even within an armed conflict but does not reach the threshold of an 'attack' under the law of war, it would be misguided to subject such an operation to the strict application of the targeting principles. This argument applies regardless of the specific conceptualisation of the term 'attack'. Even under the loose conception, according to which reversible cyber operations seeking to disable objects qualify as attacks,[86] some cyber operations still manifestly fall outside of the scope of the law of war. This would be the case, for instance, with respect to the dissemination of propaganda by cyber means or to operations tantamount to economic sanctions.[87]

In such circumstances, to insist on the applicability of the law-of-war principles of targeting would be misplaced and could in fact result in a reduction of humanitarian protection. By way of illustration, let us consider the example of interfering with a civilian television broadcast during an armed conflict. There is a general consensus that an operation consisting solely of temporarily blocking a television broadcast would not amount to an 'attack' under the law of war.[88] Yet if principles of targeting were to be applied to a cyber operation aiming to disrupt the transmission of television signal, the operation would highly likely fail to live up to the principle of distinction. This is because its target, specifically the communications system supporting the television broadcast, would normally be civilian in nature and as such it would not meet the criteria of a military objective.[89]

However, the principle of distinction along with other targeting principles flows from the equilibrium between the two opposing considerations of military necessity and humanity. Once these underlying 'driving forces'[90] are taken out of the equation, the reliance on the principles may in fact result in overall detriment. This is apparent when we contrast two recent examples of targeting TV stations, one kinetic, the other one digital.

The 'kinetic' example is the 1999 NATO bombing of the Serbian state-owned TV station in Belgrade, which took the station off the air for about six hours[91] and resulted in the death of sixteen civilians.[92] Kinetic bombing is manifestly an attack under the framework of the law of war. Hence, NATO sought to justify the bombardment by describing the TV station as part of the enemy's Command, Control and Communications (C3) military network as well as of its propaganda machinery used to control the population—and as such a legitimate military objective.[93] In a later report, a committee at the International Criminal Tribunal for the former Yugoslavia (ICTY), expressed some doubts about this justification,[94] but nonetheless

86 See text corresponding to notes 67–68 above.
87 See, e.g., Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533, 559–560.
88 Schmitt (n 69) 203 fn 63; Droege (n 87) 560; *Tallinn Manual 2.0* (n 45) 418.
89 Article 52(2) AP I.
90 Dinstein (n 83) 8.
91 'Bombed Serb TV back on air' *BBC News* (23 April 1999) <http://news.bbc.co.uk/1/hi/world/europe/326339.stm>.
92 'NATO challenged over Belgrade bombing' *BBC News* (24 October 2001) <http://news.bbc.co.uk/1/hi/world/europe/1616461.stm>.
93 NATO, Press Conference by NATO Spokesman, Jamie Shea and Colonel Konrad Freytag, SHAPE (23 April 1999) <http://www.nato.int/kosovo/press/p990423l.htm>.
94 ICTY, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (14 June 2000) <http://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal> [75]–[76].

recommended against commencing an investigation related to the incident.[95] Be that as it may, from a humanitarian perspective, the civilian deaths pose a grave collateral effect of the operation that cannot be ignored.

In contrast, one may consider the 'digital' example of the 2015 cyber attack against the French network TV5 Monde. (For the purposes of this paper, we put aside the vexing question of attribution of the operation and focus solely on its impact in order to contrast it with the kinetic attack described above.[96]) Essentially, the only direct effect of the operation was to block broadcasting by the TV5 Monde network on 12 channels for approximately 10 hours.[97] If the operation had taken place in the context of an armed conflict, it would not have risen to the level of an 'attack'. However, all targeted systems were civilian in nature; therefore, the operation would by definition fall short of the principle of distinction. Although an operation of this kind does not lead to any civilian casualties, to subject it to the law-of-war targeting principles would thus render it unlawful.

This results in a paradox. A state aiming to disrupt the television signal of a station on enemy territory may be faced with a difficult dilemma. It may either engage in a kinetic attack, which might be justified along the same lines of reasoning advanced by NATO in the example above, but which will almost certainly result in civilian deaths. Alternatively, it may choose to disable the TV broadcast by way of a cyber operation, but the application of targeting principles might mean that such conduct would become internationally unlawful. In this situation, the state may well choose the 'legally safe' option, even if it would entail more human suffering.

The same logic applies to cyber operations that take place outside of any armed conflict. It may well be that an operation against a TV broadcaster in peacetime amounts to a violation of sovereignty of the territorial state, to a prohibited harmful interference, or even to a prohibited form of intervention. But this does not follow from the civilian status (*vel non*) of the target in question. The lawfulness of such a cyber operation must be determined by the application of the relevant rules,[98] but it would be misplaced to draw these directly from principles that have evolved in a different normative context and which reflect the specific aims of the law of war.

5. CONCLUSION

The 'year of the hack' confirmed the ubiquity of cyber security threats posed by malicious actors in cyberspace. In the meantime, states are slowly accepting the need to articulate international regulatory responses.[99] Against this backdrop, three overarching conclusions may be drawn from the preceding analysis. Firstly, a systemic shift has taken place, moving the regulatory focus from the law of war to general international law. A better understanding of this trend should alleviate some of the fears of fragmentation of international law and inform the debate about the relationship between the law at the vanishing point and at the core of international

95 Id. [79].

96 On that question, see further Graham Cluley, 'TV5Monde Attack Proves Hacking Attribution Is Very Difficult' (10 June 2015) <https://www.grahamcluley.com/tv5monde-attack-hacking-attribution>.

97 'How France's TV5 was almost destroyed by "Russian hackers"' *BBC News* (10 October 2016) <http://www.bbc.co.uk/news/technology-37590375>.

98 See *Tallinn Manual 2.0* (n 45) 17–27 (violation of sovereignty), 294–298 (prohibition of harmful interference), 312–327 (prohibition of intervention).

99 See, e.g., Egan (n 49) 7.

law. Secondly, this trend has allowed for specific concepts to migrate from the law of war where they had originated, evolved or consolidated and to influence other areas of international law. An illustrative example is the functionality test, which offers significant utility for the law of state sovereignty as well as the law of arms control and disarmament. Thirdly, however, it is imperative that the unique teleological underpinning of the law of war is taken into account before introducing its rules and principles to different normative contexts. Paradoxically, a blanket transplantation of these norms might in practice jeopardise the underlying humanitarian considerations.

ACKNOWLEDGEMENTS

I am thankful to Rogier Bartels, Ana Beduschi, Charles Garraway, Michael N Schmitt, and the anonymous reviewers for their valuable comments and suggestions on earlier drafts of this paper. Any remaining errors or omissions are my own responsibility.